(12) UK Patent Application (19) GB (11) 2 361 153 (13) A

(43) Date of A Publication 10.10.2001

(21) Application No 0008276.8

(22) Date of Filing 04.04.2000

(71) Applicant(s)
Global Knowledge Network Limited
(Incorporated in the United Kingdom)
Suite 94, 2 Lansdowne Row, Mayfair, LONDON,
W1J 6HL, United Kingdom

(72) Inventor(s)
Simon Alan Spacey

(74) Agent and/or Address for Service
Brookes Batchellor
102-108 Clerkenwell Road, LONDON, EC1M 5SA,
United Kingdom

(51) INT CL[7]
G06F 17/30 // H04L 9/00 29/06

(52) UK CL (Edition S)
H4P PPEB

(56) Documents Cited
EP 1033854 A2 WO 00/46952 A1 WO 00/01108 A2
US 5915087 A US 5835087 A US 5781550 A
US 5245656 A

(58) Field of Search
UK CL (Edition S) H4P PPA PPEB PPEC
INT CL[7] G06F 17/30 , H04L 9/00 12/28 29/06
Online Databases: WPI, EPODOC, JAPIO

(54) Abstract Title
User security, privacy and anonymity on the Internet

(57) A client accesses a destination sewer over the Internet through an intermediary or proxy sewer. The intermediary sewer receives the client request over a secure encrypted connection, transforms it into a standard request and forwards it to the destination sewer. The request then appears to originate from the intermediary server. Thus logging of client identity and client transactions is prevented. The intermediary sewer transforms the response and further links or references therein into a response from the intermediary site before sending it to the client. Secure email may also be sent without disclosing the sender, receiver or content.

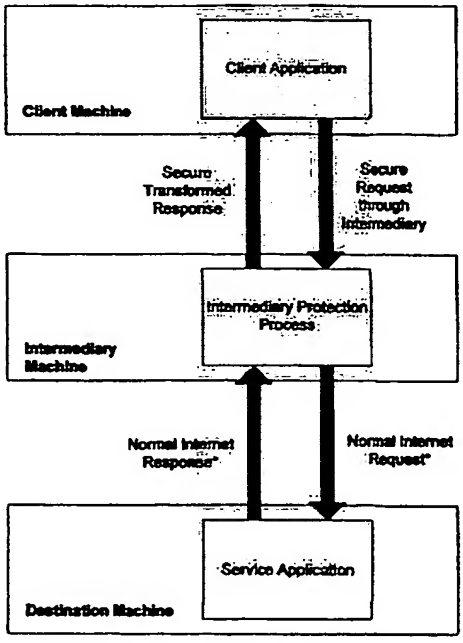


FIGURE 3

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

The claims were filed later than the filing date but within the period prescribed by Rule 25(1) of the Patents Rules 1995.

GB 2 361 153 A

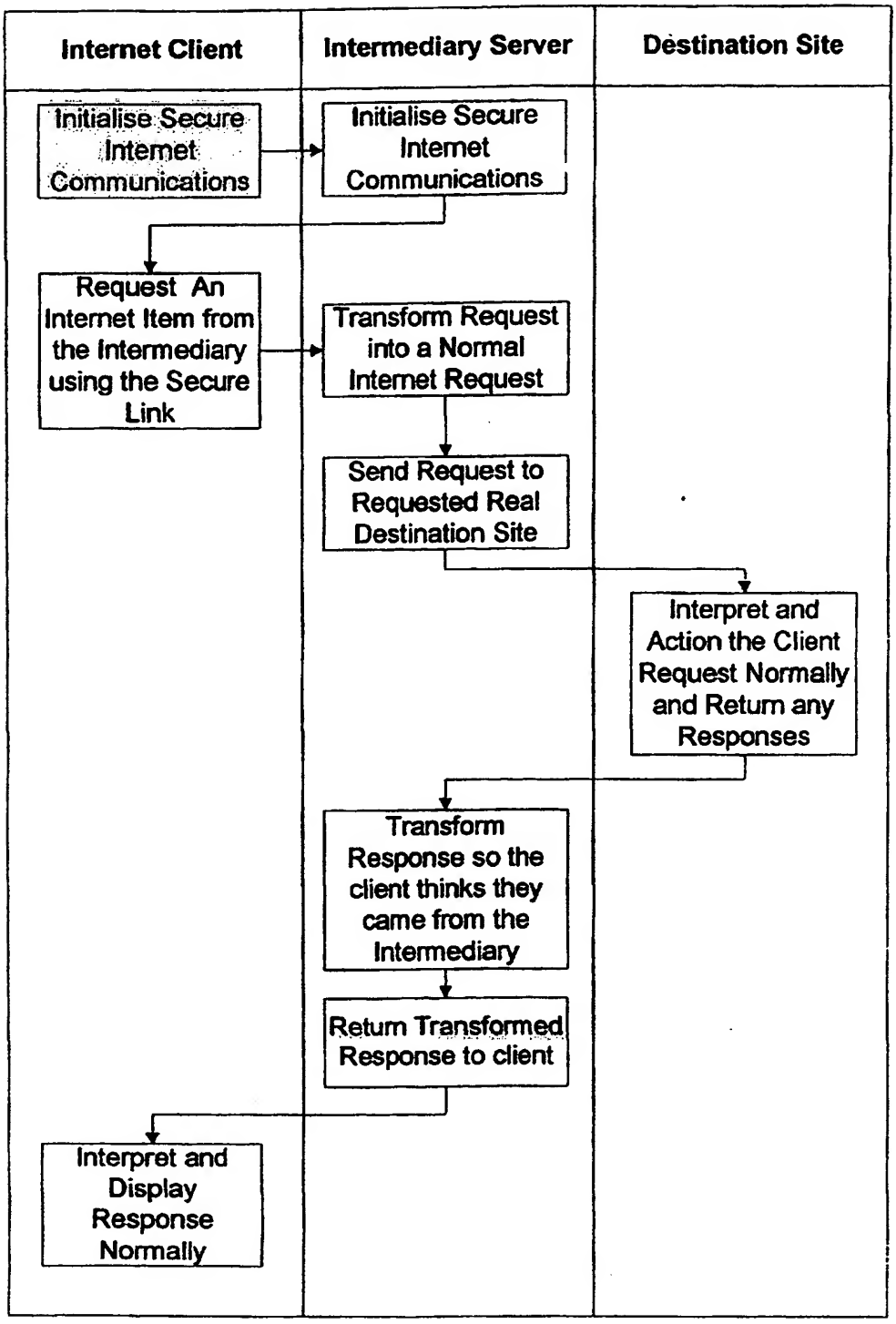

Internet Client
Intermediary Server
Destination Site
Initialise Secure Internet Communications
Initialise Secure Internet Communications
Request An Internet Item from the Intermediary using the Secure Link
Transform Request into a Normal Internet Request
Send Request to Requested Real Destination Site
Interpret and Action the Client Request Normally and Return any Responses
Transform Response so the client thinks they came from the Intermediary
Return Transformed Response to client
Interpret and Display Response Normally

FIGURE 1

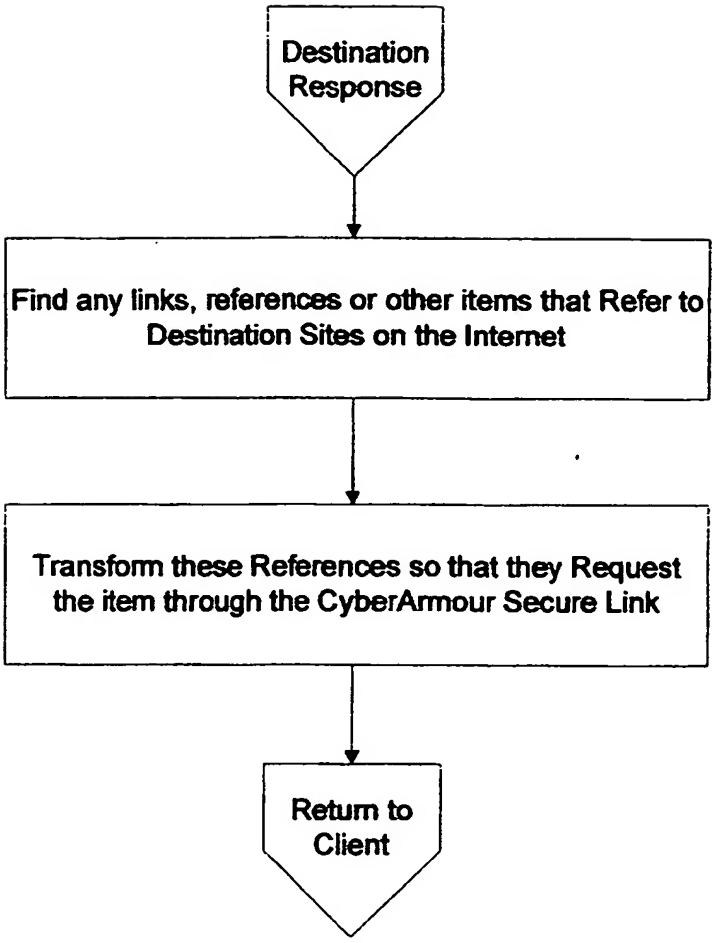
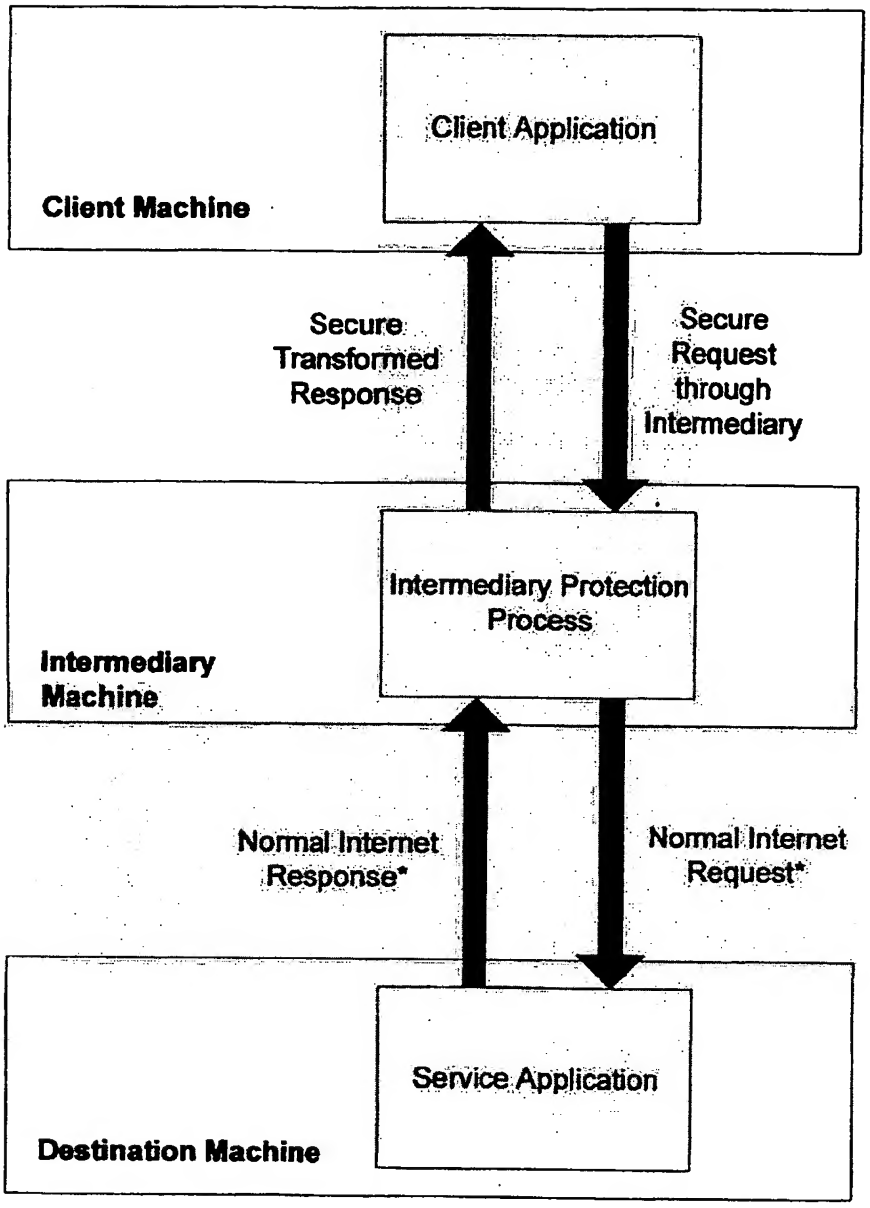

Destination Response
Find any links, references or other items that Refer to Destination Sites on the Internet
Transform these References so that they Request the item through the CyberArmour Secure Link
Return to Client

FIGURE 2



* Potentially Secure Internet Communication Depending on Destination Site and Client Request

FIGURE 3

METHODS AND APPARATUS USABLE WITH OR APPLICABLE TO THE USE OF THE INTERNET

This invention relates to methods and apparatus affording user security, privacy and anonymity on the Internet and World Wide Web.

Hypertext Transfer Protocol (HTTP) is the Internet Application Protocol most widely used on the World Wide Web. HTTP is used by a web browser as a client program to make requests of Web servers through the Internet. A web browser user can request or open a web page by typing in a Uniform Resource Locator (URL) or by clicking on a hypertext link. The browser then sends the HTTP request to the Internet Protocol (IP) address indicated by the URL or link and the requested page is returned. There are many other Internet Application Protocols such as those used for e-mail (SMTP, POP) and file transfer (FTP) as well as proprietary application protocols which are used by Internet applications beyond simple web browsers. HTTP and most other Internet Application Protocols are not secure or encrypted in any way. This means that normal Internet transactions can be easily monitored or tampered with as they pass through the Internet.

When users access the Internet using HTTP or any other Internet protocol, they access the Internet through an Internet provider of some sort. This provider may be their employer, an Internet Café, their own Internet Service Provider (ISP) or some other provider. The user's Internet provider passes the user's request on to the

destination Internet server identified by the URL and associated IP address through routers and other machines that form part of the Internet infrastructure.

User's Internet providers often log the Web Servers and URLs a user visits. These logs are in addition to history files and cookies kept locally on the user's workstation or PC and many users may object to this logging as a breach of their privacy.

In addition to this, the Internet provider and the other routers and machines that form part of the Internet, can often view the entire contents of any of the user's normal insecure Internet transactions. This can include any e-mails picked-up or sent by the user (either using the Web or a mail application) and any forms that the user fills in with personal or financial information on the Internet. The process of viewing Internet transactions as they pass through an Internet provider, router or other machine is called 'sniffing' and is widely available. The ability for Internet providers and other machines to monitor the user's Internet transactions like this further adds to fears of Cyber-Crime and breaches in security and privacy on the Internet.

Anonymity is an additional factor of concern on the Internet. Internet requests often hold in them some information about the requestor. This is often below the Application Protocol Layer and in the case of HTTP Web Browser transactions is at the socket or transport layer. Examples of this information include the Internet Address of the requestor/ user so that the Web Server can return information to them, information about the user's operating system or browser type as well as more

sensitive information. It is possible for destination Internet servers that the user contacts to log this information and use it to breach the user's anonymity.

It is a general object of the present invention to provide methods and apparatus capable of affording security, privacy and anonymity on the Internet. It is also an object of the present invention to provide such methods and apparatus that are compatible with most Internet applications including existing Web browsers.

According to an aspect of the invention there is provided a method of using the Internet which actively prevents any logging by Internet servers, providers, routers and other machines associated therewith of details of destination sites visited by a user or client and preferably, at least, hinders Internet Transaction 'sniffing' on insecure Internet transactions. The method also protects the anonymity of Internet users.

The method may involve a user/ client establishing, preferably through an Internet provider, a connection with an intervening or intermediary site, the intermediary site then provides access to destination sites for the client without the destination sites being logged as having been accessed directly by the client. The only Internet activity of the client that can be logged by any Internet servers, providers, routers and other machines associated therewith is the access to the intermediary site by the client. By using an intermediary site, the method additionally prevents logging by the end destination sites of information as to the identity of the client.

Further, the connection between the client and the intermediary site is preferably a secure, encrypted connection to hinder Transaction 'Sniffing' and further facilitate client Internet privacy. The client to intermediary site connection is preferably secure even if the corresponding client to end destination site would otherwise not be capable of a secure connection. Such a secure connection ensures encryption protection of user requests and responses, information sent through the Internet by the user (this includes the URL of the real destination site the user accesses) and information sent back to users. An example of an encrypted connection is a Secure Socket Layer (SSL) connection. SSL connections provide a public-key encryption framework widely considered to be suitable for commercial exchange and data transferral and are considered secure. SSL encryption capabilities are built in to many Web browser clients today. Using SSL, web browser requests are sent to the intermediary server using HTTPS (Secure Hyper-Text Transfer Protocol) instead of standard HTTP and these requests are transformed and passed on to the destination server using either standard HTTP or HTTPS depending on the secure capabilities of the final destination Web Server.

Preferably in the method of the invention:

1) A client establishes a secure connection with an intermediary site;
2) The client uses the secure connection to send a request for a destination site through the intermediary site;
3) The intermediary site transforms the request into a standard Internet request containing only selected information as to the direct identity of the client;
4) The intermediary site sends the Internet request to the destination site;

5) The destination site returns the requested response to the intermediary site;
6) The intermediary site transforms the response, and preferably any further links or references therein, into a response identified as being from the intermediary site; and
7) The intermediary site, using the secure connection, sends the response back to the client.

The user can read and process the returned destination site information normally and then make a request for another destination site item. To do this the user can simply enter another URL constructed in such a way that it is interpreted through the intermediary site. However, in the case of a Web browser, the user may wish to click on a hypertext link within a viewed web page. Thus, in a practical implementation of the method of the invention, as well as transforming the response into a response identified as being from the intermediary site, the intermediary site finds any references (links or other items) that refer to destination sites on the Internet; and transforms these references so that any future request made by the client using these references is made through the intermediary site. Thus the Web browser client can use the Internet securely, privately and anonymously through the, preferably secure, intermediary server by either inputting URLs directly or by clicking transformed links on web pages in a browser in the normal way to select destination sites through the intermediary server. This transformation process means that Web browsers do not need any configuration changes (such as setting their proxy server to the intermediary server), or any additional software in order for their communications to be 'locked' through the, preferably secure, intermediary server.

Client programs use ports/ sockets to connect to server programs. Port numbers range from 0 to 65535 with numbers 0 to 1023 used for standard services, for example number 80 is used as the default for HTTP and number 443 for HTTPS Web Servers. These defaults do not have to be used and preferably in the method of the present invention non-standard port numbers, i.e. above 1023, are used when establishing connection with the intermediary site. This allows clients to use communications, particularly SSL communications, through existing company or cyber-café firewalls without any reconfiguration. Internet firewalls often stop SSL communications within the standard 0 to 1023 range and are effectively bypassed by using these non-standard port numbers allowing a method, in accordance with the invention, to be used with a variety of firewalls. A method to bypass Internet firewalls using Internet port numbers above 1023 is therefore provided.

Another aspect of the invention provides a method for preventing "Denial of Service attacks" on the intermediary and destination Internet Sites. These attacks are often caused where a malicious client application repeatedly and rapidly sends requests to a destination site but does not wait for the responses. By doing this, the destination site is slowed down because it is continually sending a large number of (potentially large) Internet responses to the malicious client and has no time to service other client's requests. By keeping track of whether clients wait to receive the responses to their requests or not the intermediary server can address these "Denial of Service attacks". Preferably the method comprises holding back the passing on of client requests to the destination site by some period of time, the length of which is related

to the number of times the client has not been present to receive responses for the requests it has sent in the past.

Another aspect of the invention provides a method of sending or receiving an e-mail which actively prevents any logging by Internet servers, providers, routers and other machines associated therewith of details of the destination of the e-mail or its contents. The method may involve the client establishing preferably through an Internet provider a secure, encrypted connection with an intermediary site and sending or receiving an e-mail through the intermediary site. The only activity of the client that can be logged by any Internet servers, providers, routers and other associated machines is the access to the intermediary site by the client.

Another aspect of the invention provides a method of securely storing files on the Internet. The method comprises the client establishing preferably through an Internet provider a secure, encrypted connection with a file storage site through the intermediary server, the client sending a file to the site through the secure connection with the intermediary server and the site storing the file. In the preferred implementation of this method, the intermediary site offers the services of the file storage site itself for the user – removing the need for a second machine and second file transfer. The client can then securely save and retrieve the files by connecting to the secure intermediary site at any time.

According to another aspect of the invention there is provided a method of establishing Internet communication between a client and any normal Internet

destination site by initiating a request containing address information and interposing an intervening site between the client and the destination site, the intervening site acting to ensure that the only recordable information concerning the identities of both the client and destination site is held by the intervening site.

Another aspect of the invention provides a method affording privacy and anonymity on the Internet, the method comprising:

1) A client establishing a secure connection with an intermediary site;
2) The intermediary site offering a range of services to the client; and
3) The client selecting a service.

The services may include using existing external (normal) Internet sites and services while any logging of details of destination sites visited or contents of Internet transactions is actively prevented by the secure layer and the intermediate server, sending or receiving e-mail while any concurrent logging of the destination/ source or contents of the e-mail is actively prevented, and/or storing files securely on the intermediary site. The secure connection established between the client and intermediary site provides communication privacy over the intermediary site's services.

Another aspect of the invention provides a method of establishing an Internet or Internet-type communications link between a client or user site and a destination site for the passage of information therebetween. The method is characterised by interposing an intermediary site between the client or user site and the destination

site. The intermediary site acts as a virtual (and preferably secure) destination site for the client or user site and as a virtual client or user site for the destination site. This is to the extent that all logging entries on the destination site only show the intermediary site as the client or user and all logging entries on the client or user site only show the intermediary site as the destination site.

The methods described herein can improve efficiency and speed of Internet transactions. This can be by the use of compression and other methods. Compression is particularly important for increasing the efficiency of the client connection to the Internet as this is usually relatively slow. Thus the introduction of an intermediary server that compresses transactions as they pass to and from the client is another aspect of the invention. This can be achieved by using compressed SSL communications where the client would otherwise use uncompressed Internet connections.

According to another aspect of the invention there is provided apparatus for performing any one or more of the methods of the invention. Preferably the apparatus comprises a server connected or connectable to the Internet, the server having means to allow a client to establish a secure connection with the server. The server may comprise means to perform any of the steps of any of the methods described herein.

The invention may be understood more readily and various other aspects and features of the invention may become apparent from consideration of the following description.

Implementations and embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a flow chart illustrating the implementation of a method of the invention;

Figure 2 is a flow chart illustrating a general transformation procedure used in the implementation of a method of the invention; and

Figure 3 is a block diagram illustrating an embodiment of the apparatus of the invention in use.

Figure 1 shows the steps taken by an Internet client, an intermediary site and a destination site. A secure Internet connection or link is established between the Internet client and the intermediary site by the Internet client and then the intermediary site initialising a secure Internet communication. In the case of a Web Browser client, a HTTPS connection provides this secure link. The Internet client, using the secure link, requests an Internet item from the intermediary site. A common example of an Internet item is a normal insecure web page from a destination site. The intermediary site transforms the request into a normal Internet request suitable for the destination site to understand - such as a HTTP or HTTPS

request in the case where the destination is a normal Web Server. The normal Internet request, since it is sent by the intermediary site, contains information concerning the identity of the intermediary site and no information or only limited information concerning the identity of the real Internet client. The intermediary site sends the normal Internet request to the destination site containing the Internet item. The destination site interprets and actions the request normally and returns any response to the intermediary site as the site that requested the item. The intermediary site transforms the response to be identified as originating from the request sent to the intermediary site and using the secure link returns the transformed response to the client. The client interprets and displays the response normally. The client can use a similar secure link to make subsequent requests that are similarly processed. The only information relating to Internet activity that can be logged or monitored by a local server or ISP is the accessing of the intermediary site by the client. Importantly, since the client communicates with the intermediary site over a secure link, it is not possible for any Internet servers or the client's ISP to monitor the Internet transaction's contents or even to log the final destination URL the client requested (securely) from the intermediary site.

As well as transforming the response to be identified as originating from the request sent to the intermediary site, the intermediary site performs additional response transformations to Internet items returned from the destination site. The additional response transformations are both client specific and implementation specific and indeed may not be required in some instances and for some application protocols. Figure 2 illustrates an example additional transformation procedure. The

intermediary site locates any links, references or other items that refer to real Internet sites and transforms these so that any requests made for these links are requested via the intermediary site. The intermediary site then returns the transformed response to the Internet client. This 'locks' future requests through the (preferably secure) intermediary site. For example, a Web Browser user can click on a hypertext link within a viewed web page to access a separate web page. The web page is accessed through the intermediary site (following the steps of the method described with reference to Figure 1) rather than directly because the link has been transformed. Direct access, through an untransformed link, would result in the link to the Internet via the intermediary site being broken and normal web access resuming which could be logged or monitored by Internet servers or the user's ISP.

A specific potential transformation of part of a Web site's response is shown below for illustration purposes. A response returned by the destination site to the intermediary site, www.cyberarmour.com, defines a link to another web site, www.gkn.net. The corresponding HTML code segment containing the response is:

<A HREF="http://www.gkn.net">

This line of HTML code is located and transformed to:

<A HREF="https://www.cyberarmour.com:2030/Encrypted:www.gkn.net">

All other references, links and other Internet items would be similarly changed before the response is returned to the client. The word "Encrypted:" and the ":2030" port number are implementation dependent and could be omitted or changed. The

non-standard port number of 2030 has been included here to by-pass Internet firewalls and consequently avoids any potential need for client or firewall reconfiguration. This example transformation is constructed to ensure that when the user clicks on the link generated from the code segment, a request is sent through a secure connection (https://) to the intermediary server (www.cyberarmour.com) bypassing any firewalls (:2030) and requests from the intermediary server the normal HTTP (Encrypted:) Web Server item 'www.gkn.net'.

A preferred embodiment/ implementation, shown in Figure 3, requires no change to the client or destination server components. This implementation is suitable for client applications that have existing secure communication capabilities such as most Internet/ Web Browsers. The client application connects securely to the intermediary server and requests a connection to a destination server through this secure link. The intermediary server transforms the request into a normal Internet request and sends it to the destination server on a "stream" basis. Destination responses are transformed where necessary to force any external links and references to be via the intermediary server (using a general process based on the method described with reference to Figure 2). The transformed responses are also returned to the client on a stream basis.

Using a stream basis the client requests and destination responses are passed/ streamed through the intermediary server as they arrive. Advantageously, no extra client or destination server components or changes are required and no client or destination server speed penalties are seen.

Alternative implementations of the method are also envisaged. For instance, it is possible to pass the data through the intermediary server as a "batch" operation as opposed to on a "stream" basis. The intermediary server would wait to transfer certain whole portions of requests and responses instead of as they arrive. To speed up this process, the intermediary site may cache the transformed requests and responses. Also, multi-stage variations could be used where requests and responses are treated as whole or partial files rather than streams with tasks performed on a batched basis rather than a real-time basis which processes the data as it arrives.

It is also possible to include additional components on the client or destination server machines. These components may be for the provision of secure communication capabilities and/or for performing part of the intermediary site procedures on the client or destination server machine. Various optimisations such as compression and securing the intermediary to destination site connection can also be implemented in this manner. It is also possible to alter some client and destination components to remove the need for link and reference transformations. This includes setting the intermediary server as a web browser's Proxy Server. It is also possible to distribute the intermediary server process across several intermediary servers.

Those skilled in the art will appreciate that there are numerous potential implementations within the scope of the invention as described.

CLAIMS

1. A method affording privacy or anonymity on an Internet-type or other Communications medium, the method comprising:
   a) establishing a secure connection between a client and an intermediary site; and
   b) offering or providing one or more services through or on the intermediary site to the client.

2. A method as claimed in claim 1, wherein the services include using the intermediary site to forward communications between the client and destination sites so as to prevent one or more of the following:
   a) any logging of details of the true destination sites the client has visited by machines capable of monitoring client transactions by means of the secure client-intermediary connection;
   b) any logging of the contents of transactions between clients and destination sites by machines capable of monitoring client transactions by means of the secure client-intermediary connection;
   c) destination sites finding-out the true origin or location of clients by means of formatting client requests to giving the destination site the impression that the intermediary site was the origin of the communication.

3. A method as claimed in claim 1 or claim 2, wherein the services include one or more of the following:
   a) accessing of destination Internet sites by the client through the secure connection with the intermediary site and actively preventing any logging by Internet servers, providers, routers or other machines associated therewith that the destination sites have been visited by the client;
   b) sending or receiving e-mails while any logging of either the destination, source or contents of the e-mail is actively prevented;
   c) storing files securely on the intermediary site;

d) transferring messages between multiple clients connected through the intermediary as in a secure telephone, conferencing, Internet "Chat", "Message Board" service or similar.

4. A method as claimed in any one of claims 1 to 3 and further comprising:
   a) accessing of destination Internet or Internet-type service sites by the client through the secure connection with the intermediary site; and
   b) actively preventing any logging by Internet servers, providers or other machines associated therewith that the destination sites have been visited by the client.

5. A method as claimed in any of the previous claims and further comprising:
   a) establishing the secure connection between the client and the intermediary site;
   b) allowing the client to use the secure connection to send a request to the intermediary site for forwarding to a destination site;
   c) transforming the request into a standard request that can be interpreted by the destination site as originating at the intermediary;
   d) sending the transformed client request from the intermediary to the destination site or a proxy for that site;
   e) receiving the requested response from the destination site at the intermediary;
   f) transforming the destination response into a response identified as being from the intermediary site; and
   g) using the secure connection to return the response back to the original client.

6. A method as claimed in claim 5 and further comprising the step of transforming links and references in the response so that any future request made by the client based on the response from the destination site is made by the client through the intermediary site not directly to the destination site.

7. A method as claimed in any one of claims 1 to 6 and further comprising the intermediary site checking that a client connection remains open to the intermediary throughout a

communication transaction so that destination responses can be delivered to the client and that the client is not attempting an anonymous denial of service attack on the destination site.

8. A method as claimed in any one of claims 1 to 5 and further comprising:
   a) sending or receiving e-mail by the client through the secure connection with the intermediary site; and
   b) actively preventing any logging by Internet servers, providers, routers or other machines associated therewith of details of the client, e-mail content, recipients and sender.

9. A method as claimed in any one of claims 1 to 5 and further comprising sending or retrieving a file by the client through the secure connection with the intermediary site and the intermediary site securely storing or retrieving the file.

10. A method as claimed in claim 9, wherein the intermediary site itself stores the file.

11. A method as claimed in any one of claims 1 to 10 and actively hindering Internet transaction sniffing.

12. A method as claimed in any one of claims 1 to 11, wherein the secure connection is an encrypted connection.

13. A method as claimed in claim 12, wherein the encrypted connection is an SSL connection.

14. A method as claimed in any one of claims 1 to 13 used to allow communication with destination sites where the client is restricted from directly accessing the destination site by a restrictive Internet firewall, proxy server, physical limitations or other apparatus.

15. A method as claimed in claim 14 comprising the intermediary listening for client requests on Internet port numbers above 1023.

16. A method as claimed in any one of claims 1 to 15 and adapted to improve the efficiency and speed of communication transactions by either:
    a) adding compression to the client-intermediary connection
    b) utilising a rapid communications channel between the client and the intermediary so as to reduce overall round-trip or delay times between the client and ultimate destination

17. A method substantially as herein described with reference to Figures 1 to 3 of the accompanying drawings.

18. Use of any of the methods of claims 1 to 17.

19. Apparatus configured to perform any one of the methods of claims 1 to 18.

20. Means to perform any of the methods of claims 1 to 18.

The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

Application No: GB 0008276.8
Claims searched: All
Examiner: Gareth Griffiths
Date of search: 2 April 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4P (PPA, PPEB, PPEC)

Int Cl (Ed.7): G06F 17/30, H04L 9/00, 12/28, 29/06

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X,E	EP1033854 A2	(PITNEY BOWES) whole document	1-5,9,11 at least
X,E	WO00/46952 A1	(FUNDXPRESS) p.3 lines 4 - 20	1,12,13 at least
X	WO00/01108 A2	(PRIVADA) p.5 line 25 - p.12 line 10	1-5,8,11-14,16 at least
X	US5915087	(HAMMOND) abstract	1-5,7-9,11,14,16 at least
X	US5835087	(HERZ) col.31 line 23 - col.48 line 26	1-5,8-12,14,16 at least
X	US5781550	(TEMPLIN) col.3 lines 21-40	1-5,8,9,11-14 at least
X	US5245656	(LOEB) abstract	1-5,9,10,12,14 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.